WHAT IS CLAIMED IS:

1. A method of protecting a username during authentication, the method comprising:

obtaining a plain text username over a secure communication channel;

obtaining a server identifier for a server;

obscuring the plain text username using the server identifier;

providing the obscured username and the plain text username to the server; and

communicating authentication information including the obscured username over a non-secure communication channel from a client.

2. The method of claim 1, wherein the server identifier is a uniform resource locator (URL) corresponding to the server.

3. The method of claim 1, wherein the server identifier is an authentication domain corresponding to the server.

4. The method of claim 1, wherein obscuring the plain text username using the server identifier comprises encrypting the plain text username using an encryption method.

5. The method of claim 1, wherein the encryption method is advanced encryption standard (AES).

6. The method of claim 1, wherein the client is a wireless device.

7. The method of claim 1, wherein obtaining a plain text username over a secure communication channel comprises establishing an encrypted communication session between the user and the server and communicating a plain text username from the user to the server.

8. The method of claim 1, wherein the authentication information satisfies a plain text, unencrypted authentication scheme.

9. The method of claim 1, wherein the server identifier is a combination of an authentication domain and a uniform resource locator (URL) of the server.

10. A username protection process comprising:

registering a user with a selected server by requesting and receiving a plain text user identifier, creating an obscure version of the plain text user identifier, and storing the plain text user identifier and the obscure version of the plain text user identifier on the selected server; and

initiating a communication session between the user and the selected server by the communication of the obscure version of the plain text user identifier over a plain text communication channel.

11. The process of claim 10, wherein the user is a wireless client device communicating over a non-encrypted channel.

12. The process of claim 10, wherein communication over a plain text channel involves the obscure version of the plain text user identifier and communication over a secure channel can use the plain text user identifier.

13. The process of claim 10, wherein the obscure version of the plain text user identifier is stored on the user device.

14. A system for protecting a username during authentication over a non-encrypted channel, system comprising:

a client device being configured to communicate information over unsecure communication channels; and

a server having stored therein a plain text user identifier communicated by the client device over a secure communication channel and an obscured user identifier corresponding to the plain text user identifier.

15. The system of claim 14, further comprising a registration device being configured to communicate information over secure communication channels.

16. The system of claim 15, wherein the client device and registration device are the same device.

17. The system of claim 14, wherein the client device does not encrypt communication when communicating with the obscured user identifier created from the plain text user identifier.

18. The system of claim 14, wherein the client device has stored therein the plain text user identifier and the obscured user identifier.

19. The system of claim 14, wherein the obscured user identifier corresponding to the plain text user identifier is created by encrypting the plain text user identifier with a key.

20. The system of claim 19, wherein the key is based on the uniform resource locator (URL) of the server or an authentication domain of the server.